Abstract

Steganography is the science of hiding digital information in such a way that no one can suspect its existence. Unlike cryptography which may arouse suspicions, steganography is a stealthy method that enables data communication in total secrecy. Steganography has many requirements, the foremost one is irrecoverability which refers to how hard it is for someone apart from the original communicating parties to detect and recover the hidden data out of the secret communication. A good strategy to guarantee irrecoverability is to cover the secret data not using a trivial method based on a predictable algorithm, but using a specific random pattern based on a mathematical algorithm. This paper proposes an image steganography technique based on the Canny edge detection algorithm. It is designed to hide secret data into a digital image within the pixels that make up the boundaries of objects detected in the image. More specifically, bits of the secret data replace the three LSBs of every color channel of the pixels detected by the Canny edge detection algorithm as part of the edges in the carrier image. Besides, the algorithm is parameterized by three parameters: The size of the Gaussian filter, a low threshold value, and a high threshold value. These parameters can yield to different outputs for the same input image and secret data. As a result, discovering the inner-workings of the algorithm would be considerably ambiguous, misguiding steganalysts from the exact location of the covert data. Experiments showed a simulation tool codenamed GhostBit, meant to cover and uncover secret data using the proposed algorithm. As future work, examining how other image processing techniques such as brightness and contrast adjustment can be taken
advantage of in steganography with the purpose of giving the communicating parties more preferences to manipulate their secret communication.

References

Index Terms

Computer Science                Image Processing

Keywords

Image Steganography  Canny Edge Detection  Parameterized Algorithm